



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/773,665	02/02/2001	Donald B. Johnson	6944-8-1	7060

293 7590 11/02/2006

Ralph A. Dowell of DOWELL & DOWELL P.C.  
2111 Eisenhower Ave  
Suite 406  
Alexandria, VA 22314

EXAMINER

KLIMACH, PAULA W

ART UNIT PAPER NUMBER

2135

DATE MAILED: 11/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

# Office Action Summary

Application No.

09/773,665

Applicant(s)

JOHNSON ET AL.

Examiner

Paula W. Klimach

Art Unit

2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 16 August 2006.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 12-21 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 12-21 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION*****Double Patenting***

The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

6279110 B1	09773665
<p>I Claim 1. A method of signing and authenticating a message m in a public key data communication system, by a correspondent having a long term private key, d, and corresponding long term public key derived from said long term private key, d, comprising the steps of:</p>	<p>I Claim 12. A method for verifying a signature for a message m in a data communication system established between a sender and verifier, said sender having generated in a secure computer system a masked signature having a first signature component r computed using a first short term public key, derived from a first short term private key; a second signature component s computed using a second short term private key on said message m, a long term private key, and said first signature component r; and a third signature component computed using said first and second short term private keys, said method for verifying comprising said verifier:</p>

<p>II a) generating a first short term private key <math>k</math>; b) computing a first short term public key derived from said first short term public key <math>k</math>; c) computing a first signature component <math>r</math> by using said first short term public key; d) generating a second short term private key <math>t</math>; e) computing a second signature component <math>s</math> by using said second short term private key <math>t</math> on said message <math>m</math>, said long term private key <math>d</math>, and said first signature component <math>r</math>; f) computing a third signature component <math>c</math> using said first and second short term private keys <math>k</math> and <math>t</math> respectively, and sending said signature components <math>(r,s,c)</math> as masked digital signature of said message <math>m</math> to a receiver computer system associated with said secure computer system; g) using said second and third signature components <math>(s,c)</math> to compute a normal signature component <math>s'</math> and sending said signature components <math>(s', r)</math> as a normal digital signature to a receiver verifier computer system; and in said verifier ss</p>	<p>II a) obtaining a regular signature derived from said masked signature <math>(r,s,c)</math>, said regular signature having said first signature component <math>r</math>, and another signature component <math>s'</math> computed using said second signature component <math>s</math> and said third signature component <math>c</math>;</p>
---	---

III h) verifying said normal signature	
IV 2. A method as defined in claim 1 said first short term private key $k$ is an integer and said first short term public key is derived by computing the value $kP = (x,y)$ wherein $P$ is a point of prime order $n$ in $E(F_q)$ , wherein $E$ is an elliptic curve defined over $F_q$ .	III b) recovering a point on an elliptic curve defined over a finite field using said message $m$ and said another signature component $s'$ ;
V 3. A method as defined in claim 2, said first signature component $r$ having a form defined by $r = x' \pmod{N}$ wherein $s$ is derived by converting said coordinate $x$ to an integer $x'$ .	IV c) converting an element of said point to an integer; d) calculating a value $r'$ using said integer; and
	V e) verifying said regular signature $(r,s')$ if said value $r'$ is equal to said first signature component $r$ .

**Claims 12-21** are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claim 1 of U.S. Patent No. 6279110 B1. Although the conflicting claims are not identical, they are not patentably distinct from each other because the method of verifying the signature of instant application 09773665 ('665) verifies the same parameters of  $(r,s')$  using the masked signature  $(r,s,c)$  as the patent 6279110 B1 ('110) as shown in the element VI of application '665 and element III of the patent '110. Furthermore, the

Art Unit: 2135

parameters (r,s') of the instant application and the patent are derived in the same manner as shown in element II of the patent '110 and the element I of the application '665. The further steps of recovering a point from an elliptic curve and converting an element of the point to an integer of element III and IV of the application '665 are also derived in the same way as the element IV and V the patent '110

**Claim 1** of Patent 6279110 B1 contain(s) every element of claim 12 of the instant application and thus anticipate the claim(s) of the instant application. Claim(s) of instant application therefore is/are not patently distinct from the earlier patent claim(s) and as such is/are unpatentable over obvious-type double patenting. A later patent/application claim is not patentably distinct from an earlier claim if the later claim is anticipated by the earlier claim.

"A later patent claim is not patentably distinct from an earlier patent claim if the later claim is obvious over, or **anticipated by**, the earlier claim. In re Longi, 759 F.2d at 896, 225 USPQ at 651 (affirming a holding of obviousness-type double patenting because the claims at issue were obvious over claims in four prior art patents); In re Berg, 140 F.3d at 1437, 46 USPQ2d at 1233 (Fed. Cir. 1998) (affirming a holding of obviousnesstype

double patenting where a patent application claim to a genus is anticipated by a patent claim to a species within that genus). " ELI LILLY AND COMPANY v BARR LABORATORIES, INC., United States Court of Appeals for the Federal Circuit, ON PETITION FOR REHEARING EN BANC (DECIDED: May 30, 2001).

"Claim 12 and Claim 13 are generic to the species of invention covered by claim 3 of the patent. Thus, the generic invention is "**anticipated**" by the species of the patented invention. Cf., Titanium Metals Corp. v. Banner, 778 F.2d 775, 227 USPQ 773 (Fed. Cir. 1985) (holding that an earlier species disclosure in the prior art defeats any generic claim) 4 . This court's predecessor has held that, without a terminal disclaimer, the species claims preclude issuance of the generic application. In re Van Ornum, 686 F.2d 937, 944, 214 USPQ 761, 767 (CCPA 1982); Schneller , 397 F.2d at 354. Accordingly, absent a terminal disclaimer, claims 12 and 13 were properly rejected under the doctrine of obviousness-type double patenting." (In re Goodman (CA FC) 29 USPQ2d 2010 (12/3/1993)

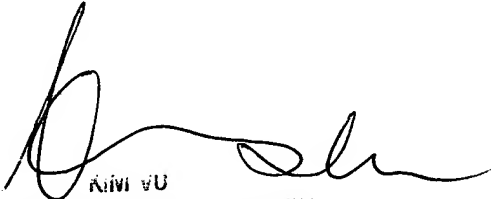
***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paula W. Klimach whose telephone number is (571) 272-3854. The examiner can normally be reached on Mon to Thr 9:30 a.m to 5:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

PWK  
Monday, October 30, 2006

  
KIM VU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100